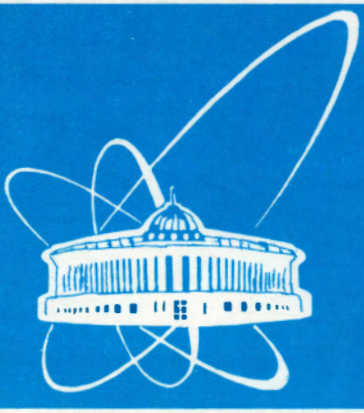

сообщения
объединенного
института
ядерных
исследований
дубна

E5-94-224

A.Yu.Zharkov [1]

INVOLUTIVE POLYNOMIAL BASES: GENERAL CASE

[1]Saratov University, Astrakhanskaya 83, Saratov 410071, Russia

1994

1 Introduction

In our recent paper [1], the notion of involutive bases of polynomial ideals was introduced and an algorithm for computing involutive bases was presented. The improved version of the algorithm together with the proof of its correctness in zero-dimensional case is given in [2]. Our computation experience [1, 2] shows that involutive bases of zero-dimensional ideals in the total-degree term ordering may be computed by this algorithm considerably faster than the reduced Gröbner bases by Buchberger's algorithm [3]. Note that involutive basis is a special form of the redundant Gröbner basis, so it gives all information about ideal and solutions. Moreover, the knowledge of involutive basis in the case of generic zero-dimensional radicals provides an effective method for converting it into the lexicographical Gröbner basis from which the solutions may be easily obtained [4].

In the positive-dimensional case, involutive bases in the sense of [1] are not sure to exist. This principle difficulty of the involutive approach is resolved in the present paper. The idea is to use more sophisticated definition of involutivity than in [1]. In our previous works [1, 2, 4] we used the involutivity conditions taken from the book of J.F.Pommaret [5]. In general case of positive-dimensional ideal, the involutive basis in the sense of Pommaret does exist only after generic linear change of variables which is not effective for practical computations. In the present paper we use another definition of involutivity coming from the works of M.Janet [6]. Unlike Pommaret bases, involutive bases in the sense of Janet exist for any polynomial ideal. We clarify the relation between Janet,Pommaret and Gröbner bases and propose an algorithm for computing Janet bases. The algorithm is implemented in the computer algebra system REDUCE [7]. It turns out that in the zero-dimensional case the new algorithm works not worse than the algorithm $INVBASE$ described in [4].

2 Pommaret Bases

Throughout this paper we use the notations:
K– arbitrary zero characteristic field;
a, b– elements of K;
$K[x_1, \ldots, x_n]$– polynomial ring over K;
f, g, h, p– polynomials from $K[x_1, \ldots, x_n]$;
F, G, H, P– finite subsets in $K[x_1, \ldots, x_n]$;
$card(F)$– cardinality (number of elements) of F;
u, v, w, s– terms in polynomials (without coefficients from K);

$deg_i(u)$– degree of variable x_i in u;
$cf(f, u)$– coefficient of u in f;
(F)– ideal generated by F.

Let $<_T$ be some admissible term ordering and let variables be ordered as $x_1 <_T x_2 <_T \ldots <_T x_n$. We denote by

$lt(f)$– leading term in f w.r.t. $<_T$;
$lc(f)$– leading coefficient in f, i.e. $cf(f, lt(f))$;
$red(f) = f - lc(f) \cdot lt(f)$;
$lt(F) = \{lt(f) \mid f \in F\}$;
$lcm(F)$– least common multiple of all $lt(f)$, $f \in F$;
$min_T(F)$– polynomial in F with minimal lt.

We recall some main concepts and results of the involution approach developed in [1, 2, 4] and based on the definition of involutivity taken from [5].

Definition 1 [5]. Variable x_i is *multiplicative in the sense of Pommaret* for the term u if its index i is not greater than the index of the lowest variable in u. Otherwise, x_i is *non-multiplicative in the sense of Pommaret* for the term u.

For a given polynomial g we denote by $NM_P(g)$ a set of non-multiplicative variables for $lt(g)$.

Definition 2. The term u is a *Pommaret divisor* for the term w if $w = u$ or $w = u \cdot v$, $v \neq 1$, where all variables contained in v are multiplicative for u (symbolically $u \leq_P w$).

Definition 3. The polynomial h is a *Pommaret normal form* of polynomial f modulo G (symbolically $h = NF_P(f, G)$) if $h = f + \sum_{ij} a_{ij} g_i \times u_{ij}$ where $g_i \in G$, $a_{ij} \in K$, all variables in each term u_{ij} are multiplicative for $lt(g_i)$ and no one term in h has a Pommaret divisor in $lt(G)$.

In contrast to the Pommaret normal form, we denote by $NF(f, G)$ an usual normal form of f modulo G. An algorithm for computing NF_P may be obtained from one for NF [3] replacing usual division of terms by division in the sense of Pommaret.

Definition 4. G is *autoreduced in the sense of Pommaret* if

$$\forall_{g,g' \in G, g \neq g'} \neg(lt(g) \leq_P lt(g')).$$

G is *completely autoreduced in the sense of Pommaret* if $\forall_{g \in G} NF_P(g, G \setminus \{g\}) = g$

Definition 5 [5]. G is an *involutive basis in the sense of Pommaret (Pommaret basis)* if it is autoreduced in the sense of Pommaret and

$$\forall_{g \in G} \forall_{x \in NM_P(g)} NF_P(g \cdot x, G) = 0 \qquad (1)$$

The main properties of Pommaret bases established in [1, 2] are listed below.

Properties of Pommaret bases.

1. If G is a Pommaret basis then $\forall_{f\in(G)}\ NF_P(f,G)=0$.
2. If G is a Pommaret basis then $\forall_h\ NF_P(h,G)=NF(h,G)$.
3. Any Pommaret basis is a Gröbner basis, generally redundant.
4. If the Pommaret basis of a given ideal exists, it is unique.
5. For any zero-dimensional ideal there exists a Pommaret basis.
6. For any positive-dimensional ideal a Pommaret basis does exist after the *most* invertible linear changes of variables.

One may easily check that involutive basis in the sense of Pommaret exists not for any positive-dimensional ideal. E.g., for an ideal generated by a single polynomial f the Pommaret basis does exist if and only if $lt(f)$ is a power of the leading variable. In such "irregular" cases the algorithm for computing involutive bases developed in [1, 2] does not stop. Moreover, there are no criteria for recognizing the irregular situations a priori. This was the main difficulty of the involution approach. To overcome this difficulty we propose a new approach based on the more sophisticated concept of involutivity [6]. We shall prove that involutive bases in the new sense (the so-called Janet bases) exist for any polynomial ideal and may be constructed by a finite number of steps.

3 Janet Bases

Definition 6. Let U be a finite set of terms. The *group of terms* $[d_n...\,d_i]\subset U$ is

$$[d_n...\,d_i]=\{u\in U\mid deg_k(u)=d_k,\ k=n,n-1...i\}.$$

The number

$$ind([d_n...\,d_i],U)=max\{deg_{i-1}(u)\mid u\in[d_n...\,d_i]\}$$

is the *highest index* of the group $[d_n...\,d_i]$ in U.

Definition 7 [6]. Variable x_i is *multiplicative in the sense of Janet* for all terms of the group $[d_n...\,d_i]\subset U$ if $d_i=ind([d_n...\,d_{i+1}],U)$. Otherwise x_i is *non-multiplicative in the sense of Janet* for all such terms.

Note that in contrast to definition 1 the multiplicative and non-multiplicative variables for a given term are defined now with respect to some finite set of terms.

Definition 8. The term $u\in U$ is a *Janet divisor* for the term w if $w=u$ or $w=u\cdot v$, $v\neq 1$, where all variables contained in v are multiplicative for u in the sense of Janet (symbolically $u\cdot v=u\times v$).

Let F be a finite set of polynomials. For some polynomial h we denote by $NM_J(h,F)$ a set of non-multiplicative variables in the sense of Janet for the term $lt(h)$ with respect

to the set $lt(F)$. We write also $h\cdot u\equiv h\times u$ if all variables in u are multiplicative for $lt(h)$.

In general case there is no correlation between definitions 1 and 8: for a given set F a variable which is multiplicative in one sense may be non-multiplicative in another sense and vice versa. However, if F is autoreduced in the sense of Pommaret we have the following theorem.

Theorem 1. *Let F be autoreduced in the sense of Pommaret. Then $NM_J(f,F)\subset NM_P(f)$ for all $f\in F$.*

Proof. Consider some $f\in F$. Let $lt(f)=x_n^{d_n}...x_i^{d_i}$ where $d_i\neq 0$. We have to prove that if variable x_k is multiplicative for f in the sense of Pommaret (i.e. $k\in\{1,...,i\}$) then it is also multiplicative for f in the sense of Janet. First assume that $k=i$ and x_i is non-multiplicative for f in the sense of Janet. By definition 7 it means that there exists a non-empty group $[d_n...\,d_{i+1},e_i]\subset lt(F)$ where $e_i>d_i$. But in this case $lt(f)$ is a Pommaret divisor for all terms from this group which contradicts the fact that F is autoreduced in the sense of Pommaret. Now assume that $k<i$ and x_k is non-multiplicative for f in the sense of Janet. It means that there exists a non-empty group of the form $[d_n...\,d_i,0...0,e_k]\subset lt(F)$. Again, $lt(f)$ is obviously a Pommaret divisor for all terms from this group. Therefore F is not autoreduced in the sense of Pommaret. The obtained contradiction proves the theorem. □

Definition 9. The *prolongation* of the polynomial $f\in F$ by variable x is a product $f\cdot x$. If $x\in NM_J(f,F)$ then the prolongation is called non-multiplicative, otherwise multiplicative.

Definition 10. F is *weakly reduced* if all terms in $lt(F)$ are different.

Theorem 2. *If F is weakly reduced then for any term v there exist no more than one Janet divisor in $lt(F)$.*

Proof. Assume for a contradiction that the term v has two different Janet divisors in $lt(F)$: u and u' such that $u\neq u'$. Let $u<_L u'$ where by $<_L$ is meant the lexicographical term ordering. The latter means that there exists $i\in\{1,...,n\}$ such that

$$deg_k(u)=deg_k(u')=d_k,\ i<k\leq n, \tag{2}$$

$$deg_i(u)<deg_i(u'). \tag{3}$$

Consequently, $deg_i(v/u)\neq 0$. It is easy to observe that the variable x_i contained in the term (v/u) in non-zero power is not multiplicative (in the sense of Janet) for the term $u\in[d_n...\,d_{i+1},deg_i(u)]$ because from (2),(3) it follows that $deg_i(u)\neq ind([d_n...\,d_{i+1}],lt(F))$. It means that u is not a Janet divisor for v. The obtained contradiction proves the theorem. □

Corollary 1. *If F is weakly reduced then for all $u,u'\in lt(F)$ such that $u\neq u'$ and for all v,v' an inequality $u\times v\neq u'\times v'$ holds.*

Proof. Otherwise the term $w = u \times v \equiv u' \times v'$ would have two different Janet divisors which contradicts theorem 2. □

Below, an algorithm is described which for a given term u and a given weakly reduced set F either returns a Janet divisor of u in $lt(F)$ or reports that such divisor does not exist.

Algorithm 1.
Input: $u = x_n^{d_n}...x_1^{d_1}$, F
$e_n := min(d_n, max\{deg_n(lt(f)) \mid f \in F\})$;
for $i := n-1$ **step** -1 **until** 1 **do**
    $e_i := min(d_i, ind([e_n...e_{i+1}], lt(F)))$;
    if $[e_n...e_i] \cap lt(F) = \emptyset$
        then return 'no Janet divisors';
return $x_n^{e_n}...x_1^{e_1}$;

It is easy to observe that if Janet divisor exists it is determined by algorithm 1 uniquely, in accordance to theorem 2.

Definition 11. The polynomial h is a *Janet normal form* of the polynomial f modulo G (symbolically $h = NF_J(f, G)$) if $h = f + \sum_{ij} a_{ij} g_i \times u_{ij}$ where $g_i \in G$, $a_{ij} \in K$ and no one term in h has a Janet divisor in $lt(G)$.

Properties of Janet normal form.

1. *If G is weakly reduced then for any polynomial f of the form $f = \sum_{ij} a_{ij} g_i \times u_{ij}$ where $g_i \in G$ an equality $NF_J(f, G) = 0$ holds for any sequence of reductions.*
2. *The Janet normal form of any polynomial modulo a weakly reduced set is unique.*
3. *The Janet normal form modulo a weakly reduced set G is linear, i.e. for all f, h and for all $a, b \in K$ an equality $NF_J(a \cdot f + b \cdot h, G) = a \cdot NF_J(f, G) + b \cdot NF_J(h, G)$ holds.*

Proof. Completely analogous to the proof of the same properties of Pommaret normal form, see theorems 1,2 and 3 in [1]. □

Definition 12. G is *complete* (in the sense of Janet) if for all $g \in G$ and for all $x_i \in NM_J(g, G)$ there exist $g' \in G$ and u such that

$$lt(g) \cdot x_i = lt(g') \times u. \tag{4}$$

Theorem 3. *If (4) holds for some $g, g' \in G$, $x_i \in NM_J(g, G)$, u and $lt(g) \in [d_n...d_{i+1}, d_i]$ then $lt(g') \in [d_n...d_{i+1}, d_i + 1]$.*

Proof. Let $lt(g') \in [c_n...c_i]$. It follows from (4) that $c_k \leq d_k$ for $k = n, n-1, ..., i+1$ and $c_i \leq d_i + 1$. Assume for contradiction that there exists $j \in \{n, n-1, ..., i+1\}$ such that $c_k = d_k, ..., c_{j+1} = d_{j+1}$ and $c_j < d_j$. But in this case the variable x_j which is contained in u in non-zero power is not multiplicative for the group $[c_n...c_j]$ and, in particular, for the term $lt(g')$ because there exists the group $[d_n...d_j] \subset lt(G)$ such that $[d_n...d_{j+1}] = [c_n...c_{j+1}]$ and $d_j > c_j$. From this contradiction we conclude that $c_k = d_k$ for $k = n, n-1, ..., i+1$. Now assume that $c_i < d_i + 1$. In this case the variable x_i is contained in u in non-zero power and being non-multiplicative for the group $[d_n...d_{i+1}, d_i]$ is also non-multiplicative for the group $[d_n...d_{i+1}, c_i]$, in particular, for the term $lt(g')$. This fact contradicts (4), consequently, $c_i = d_i + 1$. □

Let $<_L$ denote the pure lexicographical term ordering. An immediate from theorem 3 is

Corollary 2. *If (4) holds for some $g, g' \in G$, $x_i \in NM_J(g, G)$ and u then $lt(g) <_L lt(g')$.* □

Theorem 4 [6]. *Let G be complete. Then*

$$\forall_{g \in G, v} \exists_{g' \in G, v'} \; lt(g) \cdot v = lt(g') \times v'. \tag{5}$$

Proof. If all variables contained in v are multiplicative for $lt(g)$ then $g' \equiv g$ and $v' \equiv v$. Otherwise, if $x_i \in NM_J(g, G)$ and $deg_i(u) \neq 0$ then, because of (4), there exists $g_1 \in G$, u_1 such that $lt(g) \cdot x_i = lt(g_1) \times u_1$. Therefore $lt(g) \cdot v = lt(g_1) \cdot v_1$ where $lt(g) <_L lt(g_1)$. Repeating the same considerations for $lt(g_1) \cdot v_1$ and acting recursively we obtain a chain of equalities

$$lt(g)v = ... = lt(g_k)v_k = lt(g_{k+1})v_{k+1} = ... \tag{6}$$

where $lt(g_k) <_L lt(g_{k+1})$. Since G is finite chain (6) contains a finite number of equalities. Let $lt(g_N) \cdot v_N$ be the last product in chain (6). We conclude that $lt(g_N) \cdot v_N \equiv lt(g_N) \times v_N$ since otherwise chain (6) could be continued. Hence $g' = g_N$ and $v' \equiv v_N$. □

Corollary 3. *If G is complete then for all $g \in G$, v there exist $g' \in G$, v' such that $g \cdot v = g' \times v' + p$ where $p \in (G)$, $lt(g) \cdot v = lt(g') \times v'$ and $lt(p) <_T lt(g) \cdot v$.*

Proof. Obvious. □

Below, an algorithm *Complete* is presented which for a given set F computes a complete set G such that $(G) = (F)$.

Algorithm 2 ($G = Complete(F)$).
Input: F
Output: G - complete set such that $(G) = (F)$
$H := \{g \cdot x \mid g \in G, x \in NM_J(g, G)\}$;
$G := F$
while $H \neq \emptyset$ **do**
    $h :=$ element from H;
    $H := H \setminus \{h\}$;
    if $NF_J(lt(h), lt(G)) \neq 0$ **then**
        $G := G \cup \{h\}$;
        $H := \{g \cdot x \mid g \in G, x \in NM_J(g, G)\}$;

Proof of the correctness of algorithm 2. Let G_i be a set G computed at the $i-$th step of algorithm 2 and let $G_{i+1} = G_i \cup \{h\}$, $h \neq 0$. Since h is a non-multiplicative prolongation for G_i, from definition 7 it follows that $deg_k(lt(h)) \leq deg_k(lcm(G_i))$ for $k = 1, ..., n$. It means that $lcm(G_i) = lcm(F)$ for all i. Therefore

$$\forall_i \; card(G_i) < card(G_{i+1}) \leq card(F^*) \tag{7}$$

where F^* is a set of all polynomials of the form $f \cdot u$ such that $f \in F$ and $lt(f) \cdot u \mid lcm(F)$. Since F^* is obviously finite, from (7) it follows that algorithm 2 terminates after a finite number of steps with some result G. It means that the termination condition $H = \emptyset$ holds that is possible if only $NF_J(lt(g) \cdot x, lt(G)) = 0$ for all $g \in G$ and for all $x \in NM_J(g, G)$. The latter is just the same as the completeness conditions (4). Hence G is complete. □

Definition 13 [6]. G is an *involutive basis in the sense of Janet (Janet basis)* if it is weakly reduced and

$$\forall_{g \in G} \forall_{x \in NM_J(g)} \; NF_J(g \cdot x, G) = 0. \tag{8}$$

Theorem 5. *Let G be involutive in the sense of Janet. Then*

$$\forall_{f \in (G)} \; NF_J(f, G) = 0. \tag{9}$$

Proof. Completely analogous to the proof of property 1 of Pommaret bases, see theorem 6 in [1]. □

Corollary 4. *Any Janet basis is a Gröbner basis, generally redundant.*

Proof. Completely analogous to the proof of property 3 of Pommaret bases, see corollary 1 in [1]. □

Theorem 6. *Let G be a Gröbner basis. Then $H \equiv Complete(G)$ computed by algorithm 2 is involutive in the sense of Janet.*

Proof. Since G is a Gröbner basis, $G \subset H$ and $(G) = (H)$ we have that H is also a Gröbner basis. Hence, for all $f \in (H)$ there exist $h \in H$ and u such that

$$f = h \cdot u + \tilde{f}, \tag{10}$$

where $\tilde{f} \in (H)$, $lt(h) \cdot u = lt(f)$ and $lt(\tilde{f}) <_T lt(f)$. Since H is complete, by corollary 3 $h \cdot u$ may be represented in the form

$$h \cdot u = h' \times u' + p \tag{11}$$

where $lt(h) \cdot u = lt(h') \times u'$, $p \in (H)$ and $lt(p) <_T lt(f)$. Substituting (11) into (10), we obtain that $f = h' \times u' + f'$ where $lt(h') \times u' = lt(f)$, $f' \in (H)$ and $lt(f') <_T lt(f)$. Taking into account that $<_T$ is noetherian and acting recursively we obtain that $NF_J(f, H) = 0$ for all $f \in (H)$. In particular, the latter implies the involutivity conditions (8). □

4 Algorithm Description

Below, an algorithm for constructing Janet basis G for an ideal generated by a given set F is presented. At each step of the algorithm the prolongation $h = g \cdot x$, $g \in G$, $x \in NM_J(g)$ with minimal w.r.t. $<_T$ product $lt(g) \cdot x$ is selected and its Janet normal form $NF_J(h, G)$ is added to the current set G. This process goes on until Janet normal forms of all non-multiplicative prolongations are equal to zero.

Algorithm 3.
Input: F
Output: G - Janet basis of (F)
$G := Autoreduce(F)$;
$H := \{g \cdot x \mid g \in G, x \in NM_J(g)\}$;
while $H \neq \emptyset$ **do**
    $h := min_T(H)$;
    $H := H \setminus \{h\}$;
    $h' := NF_J(h, G)$;
    if $h' \neq 0$ **then**
        $G := Add(G, h')$;
        $H := \{g \cdot x \mid g \in G, x \in NM_J(g)\}$;

For a given F the function $Autoreduce(F)$ returns a set G such that $(G) = (F)$ and each $g \in G$ is in a usual normal form modulo $G \setminus \{g\}$. An algorithm for computing *Autoreduce* is well-known (see [3], algorithm *ReduceAll*). The description of subalgorithm $Add(F, h)$ is given below.

Subalgorithm 1 (G=Add(F,h))
Input: F, h
Output: G such that $(G) = (F \cup \{h\})$
$H := \{f \in F \mid lt(h) \leq_P lt(f)\}$;
$G := F \setminus H$;
$G := \{NF_P(g, \{h\}) \mid g \in G\} \cup \{h\}$;
while $H \neq \emptyset$ **do**
    $h := min_T(H)$;
    $H := H \setminus \{h\}$;
    $h' := NF_P(h, G)$;
    if $h' \neq 0$ **then**
        $G_0 := \{g \in G \mid lt(h') \leq_P lt(g)\}$;
        $H := H \cup G_0$;
        $G := G \setminus G_0$;
        $G := \{NF_P(g, \{h'\}) \mid g \in G\} \cup \{h'\}$;

Termination of subalgorithm 1 may be proved in the same way as for the algorithm *ReduceAll* [3].

To prove the correctness of algorithm 3 we need the following three lemmas.

Lemma 1. *Let S be an arbitrary finite set. Any infinite sequence $\{S_i\}$ of subsets $S_i \subseteq S$, satisfying the condition $\forall_{i,k>i}(S_i \setminus S_{i+1}) \cap S_k = \emptyset$, has equal neighbour elements, i.e. there exists m such that $S_m = S_{m+1}$.*

Proof. Obvious. □

Lemma 2. *Let G be a set at some intermediate step of algorithm 3 and h be a current prolongation. Then for all $g \in G$ and for all u such that $lt(g) \cdot u <_T lt(h)$ an equality $NF(g \cdot u, G) = 0$ holds.*

Proof. Since at each step of algorithm 3 the prolongation with minimal leading term is added to G, we have that for all $g \in G$ and for all $x \in NM_J(g, G)$

$$lt(g) \cdot x <_T lt(h) \rightarrow NF_J(g \cdot x, G) = 0. \tag{12}$$

Let g be a polynomial from G, u be an arbitrary term such that the condition $lt(g) \cdot u <_T lt(h)$ is satisfied. If $u \neq 1$ we may represent $g \cdot u$ as $v \cdot (g \times w)$ where $v \cdot w = u$, all variables in v are non-multiplicative and all variables in w are multiplicative for g. Fix some variable x in v and write $g \cdot u = v_1 x(g \times w)$ where $v_1 = v/x$. Because of (12),

$$g \cdot x = g_1 \times s_1 + \sum_{kl} a_{kl} g_k \times s_{kl}$$

where $g_i \in G$, $a_{kl} \in K$ and g_1 is such that $lt(g_1) \times s_1 = x \cdot lt(g)$. From the algorithm of Janet normal form it follows that $lt(g_k) \times s_{kl} <_T lt(g_1) \times s_1$. Substituting $g \cdot x$ into the equality $g \cdot u = v_1 x(g \times w)$ we have

$$g \cdot u = v_1 \cdot (g_1 \times w_1) + \sum_{kl} a_{kl} g_k \cdot u_{kl}$$

where $w_1 = s_1 \cdot w$ and, by admissibility of the ordering $<_T$, $lt(g_k) \cdot u_{kl} <_T lt(g) \cdot u$. It is obvious that $lt(g_1) \cdot v_1 <_T lt(h)$. Consequently, if $v_1 \neq 1$, we may repeat the same process for $g_1 \cdot v_1$. Then, taking into account that $v_1 <_T v$ and acting recursively, we obtain after a finite number of steps

$$g \cdot u = g'_1 \times w'_1 + \sum_{kl} a'_{kl} g'_k \cdot u'_{kl}$$

where $g'_i \in G$, $a'_{kl} \in K$, $lt(g'_1) \times w'_1 = lt(g) \cdot u$ and $lt(g'_k) \cdot u'_{kl} <_T lt(g) \cdot u$. Repeating the same process for each item in the right hand side of the last equation and taking into account the fact that the ordering $<_T$ is noetherian, we obtain after finite number of steps

$$g \cdot u = \sum_{ij} \tilde{a}_{ij} \tilde{g}_i \times \tilde{w}_{ij}$$

where $\tilde{g}_i \in G$, $\tilde{a}_{ij} \in K$. Hence, by property 1 of Janet normal form, $NF_J(g \cdot u, G) = 0$. □

Lemma 3. *Let $<_T$ be sequential term ordering and let h_i be a prolongation which is added to G at the i-th step of algorithm 3. If there exists the term u such that $lt(h_i) <_T u$ for all i, then algorithm 3 stops.*

Proof. Assume that such term u does exist. Let G_i be G computed at the i-th step of algorithm 3. From the conditions of lemma 3 and algorithm 3 it follows that $max_T(G_i) <_T u$ for all i. It is evident that if the leading term of some polynomial was reduced during the computation of G_i then it does not occur in $lt(G_k)$ for all $k > i$. Taking into account that $<_T$ is sequential ordering (each term has only finitely many predecessors), we conclude that $lt(G_i)$ satisfies the conditions of lemma 1. Hence, there exists the number m such that $lt(G_m) = lt(G_{m+1})$. Let us show that algorithm 3 stops after computing G_m. It means that Janet normal forms of all prolongations h are equal to zero. Indeed, if there exists a prolongation h such that $NF_J(h, G_m) \neq 0$ then there are two possibilities. The first one, if $lt(h)$ is not a Pommaret divisor for all $g \in G_m$ then $lt(G_{m+1}) = lt(G_m) \cup \{lt(h)\}$. The second one, if there exists $g \in G_m$ such that $lt(h) \leq_P lt(g)$ then $lt(g)$ does not occur in G_{m+1}. In both cases we have $lt(G_m) \neq lt(G_{m+1})$. The obtained contradiction proves the lemma. □

Proof of the correctness of algorithm 3. We have to prove that for any given F algorithm 3 stops with an answer G, an involutive basis in the sense of Janet. Assume for contradiction that algorithm 3 does not stop. Let G_i be G computed at the i-th step of algorithm 3. Note that from theorem 1 and subalgorithm 1 it follows that each G_i is autoreduced in the sense of Pommaret and, consequently, is weakly autoreduced. Because of lemma 3, there exists a number m such that G_m is a (generally redundant) Gröbner basis. Let h be a current prolongation which should be added to G_m. From lemma 2, property 3 of Janet normal form and the fact that G_m is a Gröbner basis we have that for all $f \in (F)$ such that $lt(f) <_T lt(h)$ an equality $NF_J(f, G_m) = 0$ holds. Hence there are two possibilities: either $NF_J(h, G_m) = 0$ or $NF_J(h, G_m) = h'$ where $lt(h') = lt(h)$. Repeating the same considerations for each G_k with $k > m$ we conclude that after computing G_m algorithm 3 begins to work in the same way as algorithm *Complete* (without reductions of the leading terms) and consequently stops after finite number of steps. Hence the termination condition $H = \emptyset$ holds which means that the output set G is involutive in the sense of Janet. □

Remark 1. The correctness of algorithm 3 is proved under the assumption that $<_T$ is a sequential term ordering, since we used lemma 3. The case of any admissible term ordering is still to be analyzed.

Remark 2. Algorithm 3 evidently differs from algorithm *InvolutionSystem* presented in [8]. In fact, algorithm of the work [8] is equivalent to successive execution of Buchberger's algorithm and algorithm *Complete* given above.

Algorithm 3 may be considerably improved by omitting a lot of zero-redundant prolongations due to the following fact.

Theorem 7. *Let G be a set at some intermediate step of algorithm 3, $h = g \cdot x$ be a*

current prolongation such that $lt(h)$ has a Janet divisor in $lt(G)$ and let the prolongation $g' \cdot x$ with $lt(g') = lt(g)$ be already considered. Then $NF_J(h, G) = 0$.

Proof. Since g' was in G at some earlier step, from the algorithm of Janet normal form we have

$$g' = g + \sum_{ij} a_{ij} g_i \cdot u_{ij} \tag{13}$$

where $g_i \in G$ and $lt(g_i)u_{ij} <_T lt(g)$. Taking into account that the prolongation $g' \cdot x$ was already considered and the term $lt(g') \cdot x$ has a Janet divisor in $lt(G)$ we have

$$g' \cdot x = \tilde{g} \times w + \sum_{kl} b_{kl} g_k \cdot v_{kl} \tag{14}$$

where $\tilde{g}, g_k \in G$ and $lt(g_k)v_{kl} <_T lt(g')x = lt(h)$. From (13),(14) we obtain

$$h \equiv g \cdot x = \tilde{g} \times w + \sum_{kl} b_{kl} g_k \cdot v_{kl} - \sum_{ij} a_{ij} g_i \cdot u_{ij} x$$

where $lt(g_k)v_{kl} <_T lt(h)$ and $lt(g_i)u_{ij}x <_T lt(g)x = lt(h)$. Hence, by property 3 of Janet normal form and lemma 2, $NF_J(h, G) = 0$. □

An improvement of algorithm 3 based on theorem 7 consists in introducing an auxiliary set P which stores the pairs $(lt(h), x)$ for already considered prolongations $h = g \cdot x$. If the corresponding pair for a current prolongation is already contained in P and if the leading term of the prolongation has a Janet divisor in $lt(G)$, then this prolongation is zero-redundant and therefore may be omitted without computing its normal form. The improved version of the algorithm is given below.

Algorithm 4.
Input: F
Output: G - Janet basis of (F)
$G := Autoreduce(F)$;
$H := \{g \cdot x \mid g \in G, x \in NM_J(g, G)\}$;
$P := \emptyset$;
while $H \neq \emptyset$ **do**
    $h := min_T(H)$;
    $H := H \setminus \{h\}$;
    if $(lt(h), x) \in P$ **then**
        if $NF_J(lt(h), lt(G)) = 0$ **then** $h' := 0$;
    else
    $P := P \cup \{(lt(h), x)\}$;
    $h' := NF_J(h, G)$;
    if $h' \neq 0$ **then**
        $G := Add(G, h')$;
        $P := P \cup \{(lt(h'), x)\}$;
        $H := \{g \cdot x \mid g \in G, x \in NM_J(g, G)$ **and** $(lt(g \cdot x), x) \notin P\}$;

Algorithm 4 has been implemented in the computer algebra system REDUCE [7]. Our computational experience shows that the proposed improvement leads to considerable speed-up.

5 Relation between Janet and Pommaret bases

From theorem 6 follows that unlike the Pommaret basis which is unique for a given ideal (if it does exist), the Janet basis is not uniquely defined. Indeed, for a given ideal there exists an infinite set of the redundant Gröbner bases and each of them generates corresponding Janet basis by applying the algorithm *Complete*. The following theorem is to establish the relation between Pommaret and Janet bases.

Theorem 8. *Let G be a Pommaret basis and H be a Janet basis of (G) autoreduced in the sense of Pommaret. Then $lt(H) = lt(G)$.*

Proof. Let h be an element of H. Since $h \in (G)$, from property 1 of Pommaret bases follows that there exists $g \in G$ such that $lt(g) \leq_P lt(h)$. Let $lt(h) = x_n^{c_n} \ldots x_i^{c_i}$ where $c_i \neq 0$. Then $lt(g) = x_n^{d_n} \ldots x_j^{d_j}$ where $j \geq i$, $d_j \leq c_j$ and $d_k = c_k$ for $k > j$. Since $g \in (H)$, by theorem 5 there exists $h' \in H$ such that $lt(h')$ is a Janet divisor for $lt(g)$. Assume for contradiction that $lt(h') \neq lt(g)$. Then $lt(h') = x_n^{e_n} \ldots x_m^{e_m}$ where $m \geq j$, $e_m < d_m \leq c_m$ and $e_k = c_k$ for $k > m$. Consequently, variable x_m is contained in the quotient $lt(g)/lt(h')$ in non-zero power and therefore it should be multiplicative in the sense of Janet for the term $lt(h')$. But it is impossible because there exists a non-empty group $[c_n \ldots c_{m+1}, c_m] \in lt(H)$ which contains $lt(h)$. Indeed, since $e_m < c_m$, variable x_m is non-multiplicative in the sense of Janet for the group $[c_n \ldots c_{m+1}, e_m]$ and, in particular, for the term $lt(h')$. The obtained contradiction proves that $lt(h') = lt(g)$. But this implies $h' \equiv h$ since otherwise H could not be autoreduced in the sense of Pommaret. Thus, for each $h \in H$ there exists $g \in G$ such that $lt(g) = lt(h)$. It means that $G = H' \cup G'$ where $H' \cap G' = \emptyset$ and $lt(H') = lt(H)$.

Now let us prove that $G' = \emptyset$. Let g be an element of G' and $lt(g) = x_n^{a_n} \ldots x_i^{a_i}$ where $a_i > 0$. Since $g \in (H)$, there exists $h \in H$ such that $lt(h)$ is a Janet divisor for $lt(g)$. Note that $lt(h)$ can not be a Pommaret divisor for $lt(g)$ because otherwise G could not be autoreduced in the sense of Pommaret. Hence $lt(h) \in [a_n \ldots a_{j+1}, b_j]$ where $j > i$ and $b_j < a_j$. From property 1 of a Pommaret basis it follows that for all N an equality $NF_J(x_j^N \cdot g, G) = 0$ holds. Consequently, there exists $g' \in G$ such that $lt(g') = x_n^{a_n} \ldots x_{j+1}^{a_{j+1}} x_j^{c_j}$ where $c_j > a_j$ (otherwise $lt(g') \leq_P lt(g)$). By theorem 5, there exists $h' \in H$ such that $lt(h')$ is a Janet divisor (but not a Pommaret divisor) for $lt(g')$. Therefore $lt(h') \in [a_n \ldots a_{k+1}, d_k]$ where $k > j$ and $d_k < a_k$. But the variable x_k which should be multiplicative in the sense of Janet for $lt(h')$ is in fact non-multiplicative. Indeed, there exists a non-empty group $[a_n \ldots a_{k+1}, a_k] \in lt(H)$ containing $lt(h)$ such that $a_k > d_k$. The obtained contradiction proves that $G' = \emptyset$. □

Corollary 5. *Let the conditions of theorem 8 hold and let G and H be both completely autoreduced in the sense of Pommaret. Then $H = G$.*

Proof. This is an immediate from the above theorem and theorem 5 in [2]. □

It is easy to observe that the result of algorithm 3 is a Janet basis completely autoreduced in the sense of Pommaret. By corollary 5, it coincides with the Pommaret basis when the latter does exist for a given ideal. Hence in the case of generic zero-dimensional radicals the successive execution of algorithm 3 (for the total degree term ordering) and algorithm *Invlex* proposed in [4] results in a lexicographical Gröbner basis from which the roots may be easily obtained.

The experiments with algorithm 3 show that it leads to approximately the same timings as algorithm *Invbase* ([2, 4]) when the Pommaret basis exists and works reasonably fast when the Pommaret basis does not exist. Note that the generalization of the proposed algorithmic approach for the linear systems of partial differential equations is direct.

References

[1] Zharkov A.Yu., Blinkov Yu.A. Involution Approach to Solving Systems of Algebraic Equations. Proceedings of the International IMACS Symposium on Symbolic Computation (Lille, France, June 14-17, 1993), G.Jacob, N.E.Oussous and S.Steinberg (Eds.), University of Lille, France, 1993, 11-16.

[2] Zharkov A.Yu., Blinkov Yu.A. Involutive Bases of Zero-Dimensional Ideals. Submitted to Journal of Symbolic Computation.

[3] Buchberger B. Gröbner bases: an Algorithmic Method in Polynomial Ideal Theory. In: (Bose N.K., ed.) Recent Trends in Multidimensional System Theory, Reidel, 1985, 184-232.

[4] Zharkov A.Yu. Solving Zero-Dimensional Involutive Systems, Preprint JINR E5-94-48. To be published in the Proceedings of "MEGA'94" (Santader, Spain, April 5-9, 1994).

[5] Pommaret J.F. - *Systems of partial differential equations and Lie pseudogroups*, (Gordon and Breach, New York, 1978).

[6] Janet M. *Lecons sur les systémes d'équations aux deriveés partielles.* (Gauthier-Villars, Paris, 1929).

[7] Hearn A.C. REDUCE User's Manual. Version 3.4. The Rand Corporation, Santa Monica, 1991.

[8] Schwarz F. Reduction and Completion Algorithms for Partial Differential Equations. Proceedings of "ISSAC'92", ACM Press, 1992, 49-56.

Received by Publishing Department
on June 14, 1994.